STATEMENT OF

SALLIE McDONALD

ASSISTANT COMMISSIONER

OFFICE OF INFORMATION ASSURANCE AND CRITICAL INFRASTRUCTURE PROTECTION

OFFICE OF FEDERAL TECHNOLOGY SERVICE

U.S. GENERAL SERVICES ADMINISTRATION

BEFORE THE

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND GOVERNMENT INFORMATION

COMMITTEE OF JUDICIARY

UNITED STATES SENATE

MAY 22, 2001

Good morning Mr. Chairman and members of the Committee. I am Sallie McDonald, the Assistant Commissioner for the GSA, FTS, Office of Information Assurance and Critical Infrastructure Protection. I wish to thank you for the opportunity to offer testimony with regard to the National Infrastructure Protection Center (NIPC).

The Federal Computer Incident Response Center or FedCIRC, is a component of GSA's Federal Technology Service. As designated by the Government Information Security Reform Act, it is the central coordination entity for dealing with computer security

related incidents affecting computer systems within the Federal civilian agencies and Departments of the United States Government.

By definition, a "computer security incident" encompasses any violation of an established or implied security policy or statute. Incidents include but are not necessarily limited to activities such as attempts to gain unauthorized access to government systems or data, disruption of service, unauthorized use of computing resources and changes to system hardware or software without consent of the owner.

FedCIRC and the NIPC are both crucial to effective cyber defense but serve differing roles to the Federal community. FedCIRC's role is to provide incident response and handling support to agencies. When an agency reports an incident, FedCIRC works with the agency to identify the type of incident, contain any damage to the agency's system, and provide guidance to the agency on recovering from the incident. The NIPC, on the other hand, collects incident reports and is responsible for providing threat assessments, vulnerability studies, warnings, and the coordination of the Federal government's investigative response to attacks.

Effective incident analysis is a product of multiple source data collection efforts, collaboration to quantify related information, and determination of the potential for proliferation and damage. Over the past few years, a virtual network of partners has evolved. This virtual network includes FedCIRC, the National Security Agency's (NSA) Computer Incident Response Center (NSIRC), the Department of Defense's (DOD) Joint Taskforce for Computer Network Operations (JTF-CNO), industry, academia, and individual incident response components within Federal agencies. The network capitalizes on the technical strengths of each participant, their strategic placement within the national infrastructure and their access to a variety of information resources. The

fluid exchange of information from the broad spectrum of participants and the wide range of technical and analytical talents can be brought to bear collectively against known and developing threats to the nation's cyber infrastructure.

FedCIRC has established bilateral information exchange relationships with key organizations across government, industry and academia. Each of these relationships is uniquely focused to ensure that the characteristics of any incident trigger a timely and appropriate response and that those organizations responding to incidents have the necessary information to proceed effectively. Any unauthorized intrusion or otherwise malicious activity targeting a government information technology resource violates criminal statutes and must therefore involve components of law enforcement.

Upon receiving an incident report from a Federal agency, FedCIRC evaluates and categorizes the incident with respect to its impact and severity. If criminal activity is indicated, FedCIRC informs the reporting agency of the requirement to immediately contact their Inspector General or the NIPC. Should the incident appear to have originated from a foreign country, FedCIRC categorizes it as having potential national security implications and immediately contacts both the NSIRC and the NIPC. The reporting agency is subsequently notified of such action by FedCIRC. There is ongoing discussion between the NIPC and FedCIRC to improve information sharing and analytic efforts and to educate agencies of the value of rapid involvement of the NIPC when incidents occur.

FedCIRC and the NIPC routinely pool their information and skills when the escalation of an incident has the potential for widespread proliferation or damage. When requested by the NIPC, FedCIRC collaborates with multiple sources and the affected agency or agencies to gather more detailed information specific to a given incident. Cyber-

incidents involving a pending or potential investigation are jointly handled in a manner that preserves sensitive cyber-evidence without adverse impact to the affected agency's mission functions or violation of constitutional law and applicable privacy statutes.

To ensure effective communication between the NIPC and FedCIRC, a technical member of the FedCIRC staff is permanently assigned to the NIPC Watch and Warning Unit. This assignment is based on a formal agreement with the NIPC. It augments the NIPC technical staff and clearly demonstrates bilateral direct support and the "trust relationship" essential to efficient and effective operations of both organizations.

Another example of our cooperative working relationship was the sharing of a system to deliver cyber security information. FedCIRC developed an electronic dissemination capability to alert the Federal CIO community, agency security managers and network administrators on cyber threats. FedCIRC has shared this system with the NIPC in order to augment the delivery of threat alert and advisory information. FedCIRC maintains the roster of participants, updates it daily and verifies it quarterly with all agencies. With NIPC employing this delivery capability, information is delivered quickly and efficiently.

The NIPC's responsibilities and relationship with the private sector and its lead role for counter-terrorism contribute significantly to the FedCIRC's analytical ability by providing global threat information. The NIPC staff communicates information to FedCIRC, which in many cases, provides deeper insight into developing situations. Knowing the extent or pattern of incidents as they may impact a critical private sector, for example, may influence the development of an alert or advisory notice issued to government agencies.

Critical Infrastructure Protection efforts and, more specifically, those for cyber-defense are a relatively new requirement in government and in the private sector. Only recently have these efforts been singled out as a priority for Federal agencies. As government direction for reporting the occurrence of incidents has been promulgated, attempts by agencies to develop related policies and procedures have sometimes been divergent because of differing individual interpretation and misunderstanding. FedCIRC and the NIPC are working diligently to jointly assess problem areas, more clearly define agency responsibilities for reporting incidents, and working with agencies to ensure they have the proper processes and procedures in place to respond to and prevent attacks on their information systems.

Moreover, to ensure that FedCIRC's operational experiences are available to officials responsible for computer security policy, oversight, and guidance, we also work closely with the Office of Management and Budget and the National Institute for Standards and Technology.

Effective cyber defenses ideally prevent an incident from taking place. Any other approach is simply reactive. FedCIRC, the NIPC, the NSIRC, the Department of Defense and industry components realize that the best response is a preemptive and proactive approach. In order to implement such an approach, all resources must be focused on the common goal of securing the nation's critical infrastructures. FedCIRC, the NIPC, DOD, the NSIRC and others comprise a virtual team, each offering significant skills and contributions to the common defense.

Summary

Mr. Chairman, the information presented today highlights the critical and effective relationship that exists between FedCIRC and the NIPC. Though both contribute individually to critical infrastructure protection, their strength in protecting information systems government-wide lies in their collaboration and coordination efforts. I trust that you will derive from my remarks an understanding of the cyber-threat and response

issues and also an appreciation for the joint commitment to infrastructure protection of FedCIRC and the NIPC. We appreciate your leadership and that of the Committee for helping us achieve our goals and allowing us to share information that we feel is crucial to the defense of our technology resources.